移动 APP 用户隐私信息泄露风险评价指标及实证研究

田波 郑羽莎 刘鹏远 李春好
吉林大学管理学院 长春 130022

摘要:[**目的/意义**]针对移动 APP 用户隐私信息泄露日益严重的现象,分析评价隐私信息泄露风险,有利于保护移动 APP 用户隐私,促进信息平台健康发展。[**方法/过程**]分析移动 APP 用户隐私信息泄露风险,构建用户隐私信息泄露风险评价指标体系,运用网络分析法(ANP)与熵权法综合确定指标组合权重,应用模糊综合评价法对移动社交 APP 进行实证分析。[**结果/结论**]所构建的移动 APP 用户隐私信息泄露风险评价指标体系具有一定的科学性与实用性,指标体系中 APP 平台原因造成隐私泄露的风险最高,用户原因造成隐私的泄露其次。整体上用户隐私泄露风险派派最高,微信最低,但都接近中等风险。为降低移动社交 APP 用户隐私信息泄露风险,移动用户、APP 平台以及监管部门各方应当针对不同 APP 的不同情况,有侧重地采取措施。

关键词: 移动 APP 用户 隐私信息 信息泄露 风险评价 网络分析法 熵权法 模糊综合评价法
分类号: G203 TP393
DOI:10.13266/j.issn.0252-3116.2018.19.013

1 引言

近年来,移动 APP 数量急剧增长,移动 APP 用户披露的个人隐私信息数据更是大量增加,随着个人信息利用领域的不断扩大,个人信息的价值不断被挖掘,我国移动互联网用户在体验个性化服务的同时,也面临着个人信息泄露和滥用的威胁[1]。以手机 APP 为例,根据 DCCI 互联网数据中心 2017 年公布的数据,安卓系统手机应用中有 96.6% 要求获取用户隐私权限,25.3% 存在越界获取隐私权限情况。由此看来,用户在使用移动 APP 的过程中会隐藏很多潜在的信息泄露风险,而用户个人隐私信息一旦泄露,可能会给用户生活带来极大的困扰或损失,也会影响信息平台的使用及效益。为保护移动 APP 用户隐私,促进信息平台健康发展,用户隐私信息泄露的相关研究已成为近几年产业界和学术界关注的重点。

移动 APP 即移动应用服务,是针对连接到互联网业务或者无线网卡业务的智能移动终端而开发的应用程序服务。隐私是指"不显露给他人的个人信息或行为等",移动 APP 用户隐私是指用户在下载或使用移动 APP 过程中所披露的个人不愿他人知道的信息,具体包括:①个人信息,如姓名、通讯地址、电话号码、电子邮箱地址、生活状态等;②数字行为,如已浏览的信息及停留时间、看过的网页以及订购的商品等;③通信内容,包括通话记录、电子邮件、短信等[3]。

国内外学者对互联网及移动 APP 用户隐私信息泄露风险开展了相关研究。国外学者 K. Zhu 等[4]计算了移动 APP 用户隐私泄露的危险系数,并根据用户偏好与移动应用的实际情况,推出了名为 AppURank 的应用程序,来为用户推荐可安全使用的 APP,以减少隐私泄露的情况;G. Bansal 等[5]以理性行为理论和前景理论为基础,从隐私信息披露环境的敏感度和用户的个性两个方面出发,探究了移动用户在进行交易时影响信任程度与披露意愿的因素;Y. Li[6]研究了网站感知声誉和用户对网站的熟悉程度这两种情境因素对用户隐私态度和网站隐私关注之间关系的影响,并分析了隐私态度的指标及来源;B. Martínez-Pérez 等[7]针对移动健康应用程序中用户个人健康信息的安全性和隐私性,分析了欧盟和美国现行相关法律,补充了一些关于安全性和隐私性的标准和认证,并为移动健康应用程序设计者提供了建议;C. L. Miltgen 等[8]开发了一个新的综合模型,该模型中包括一个先验变量(监管知识),一个含有感知隐私监管保护、信任、隐私风险的

作者简介:田波(ORCID:0000-0003-2728-4253),教授,博士,硕士生导师,E-mail:tb_teacher@126.com;郑羽莎(ORCID:0000-0002-9238-4712),硕士研究生;刘鹏远(ORCID:0000-0002-2888-2733),硕士研究生;李春好(ORCID:0000-0001-9872-7774),教授,博士,博士生导师。
收稿日期:2018-03-18 修回日期:2018-06-10 本文起止页码:101-110 本文责任编辑:刘远颖

调节结构,两个结果变量(保护行为和监管偏好),并将感知收益的直接和调节作用加入其中,之后对该模型进行了研究和测试,证明该模型的实用性。

国内学者王晰巍等[9]对国内外新媒体环境下信息隐私的研究状况、研究热点及未来的研究趋势进行了分析比较,并以知识图谱的方式对新媒体环境下的信息隐私热点及发展趋势进行了分析;李卓卓等[10]从数据生命周期视角对国内外个人隐私信息保护的相关法规进行了研究,对移动 APP 服务协议中存在的相关问题进行了分析,并提出相应的建议;刘娇等[11]对中文 APP 与英文 APP 的“用户隐私声明”内容进行了分析比较,发现与英文 APP 相比,中文 APP 存在问题较多,对用户个人隐私保护的重视程度较低;朱光等[12]在定性分析大数据环境下网络隐私风险的基础上,采用德尔菲法构建了风险评价指标体系,并引入熵值法对指标赋以权重,最后通过实证对某社交网络服务平台的隐私风险进行了分析;王珊等[13]从法律、监管、技术 3 个方面对隐私保护研究状况进行了分析,并对大数据时代个人信息保护研究方向提出了展望;孟晓明等[14]针对社交网络大数据商业化开发的各种模式中个人隐私泄露的可能原因进行了研究,并提出了相应的个人信息保护策略;徐晓露[15]分析了移动社交网络的隐私泄露状况及其产生原因,并从多个方面研究了移动社交网络用户对个人隐私保护的关注情况,提出了一系列提高网络用户个人信息保护水平的策略建议。张秋瑾[16]构建了包含 28 个指标的云计算隐私安全风险评估指标体系,对云计算服务过程中的个人隐私安全风险进行了评价。朱义杰[17]从直接交流泄露、监听信道方式泄露、窃取方式泄露、第三方造成泄露和其他因素泄露 5 个方面出发,构建了包含 26 个二级评价指标的指标体系,对位置服务中用户隐私泄露风险进行了评估。

对上述国内外学者研究成果梳理可知,对移动 APP 用户个人隐私信息的研究多集中在平台隐私声明的合理性分析、中外隐私信息保护情况的对比以及某类网络平台的用户隐私安全、隐私关注、隐私态度、信息披露行为意愿及用户的个人隐私信息保护研究等方面。相比之下,学者们对于互联网环境下用户隐私信息泄露风险关注较多,而以移动 APP 用户为研究对象的用户隐私信息泄露风险评价却少有研究;但由于移动 APP 依托移动设备,具有移动、便携、使用频率越来越高等特点,移动 APP 用户隐私泄露风险与传统的网络用户隐私泄露风险明显有较大区别,因此本文针对移动 APP 用户隐私泄露风险的研究是有益的必要补充。

本研究建立了移动 APP 用户隐私信息泄露的风险评价指标体系,将考虑指标之间关联性的网络分析法与熵权法相结合综合确定各项指标的权重,并运用模糊综合分析法以 6 个移动社交类 APP 为对象进行了实证分析。本文在理论层面构建了移动 APP 用户隐私信息泄露的风险评价指标,在实践层面可更好地帮助移动 APP 用户识别及应对潜在的信息泄露风险,为移动 APP 开发商提供相应的参考,从而尽可能地避免或者防范用户隐私的泄露,促进移动 APP 用户隐私信息保护及信息平台的健康发展。

2 移动 APP 用户隐私信息泄露风险评价指标体系设计

2.1 评价指标体系设计依据

笔者在仔细研读了大量相关文献以后,对移动 APP 用户隐私信息泄露风险评价的相关内容进行了梳理和总结。本文将移动 APP 用户隐私泄露的风险分为 4 个方面,即用户原因导致隐私信息泄露、APP 平台(运营方)原因导致隐私信息泄露、管理方原因导致隐私信息泄露以及其他原因导致隐私信息泄露。因许多 APP 在使用时都需要连接网络,所以移动 APP 用户隐私泄露风险与网络隐私泄露风险是有交叉的,而学术界已经有了很多针对网络隐私泄露风险的研究,因而这部分指标的选取可参考较成熟的文献。邝青青[18]为了研究互联网环境下个人隐私泄露的风险,设计了一套科学合理的评价体系,本研究从中直接或稍作修改后(多数为修改后)提取出适合本文的指标,即用户原因维度中的多个移动 APP 关联使用、错误操作、不良网络使用习惯,移动 APP 平台原因维度中的内部人员恶意泄露信息、滥用信息、操作失误,管理方原因维度中的基于法律或制度要求被迫披露、监理机构直接将信息共享,其他原因维度中的备份资料、从第三方平台购买隐私信息。笔者从朱光[12]通过德尔菲法构建的社交网络隐私风险评价体系中提取出用户原因导致的移动 APP 密码设置简单、其他因素中的黑客攻击两个因素,同时查阅相关文献,依据移动 APP 特有的移动性、便利性以及更强的即时性与更高的使用频率等特点,提出了对移动 APP 针对性较强的指标:用户原因维度的移动设备丢失、不关闭移动定位功能[19]、上传过多隐私数据至网盘[20]、不使用移动隐私控制功能,移动 APP 平台原因维度的移动 APP 请求权限过

田波，郑羽莎，刘鹏远，等. 移动APP用户隐私信息泄露风险评价指标及实证研究[J]. 图书情报工作,2018,62(19):101-110.

多[21]与其他原因维度的陌生无线网络的不安全性[22]。

为进一步完善评价指标体系,笔者组织了一次焦点小组讨论,经讨论初步得出了包含4个一级指标、29个二级指标的体系,后文将介绍各指标的详细内容。

2.2 风险评价指标体系初步建立

2.2.1 用户自身原因导致用户隐私信息泄露 用户原因导致隐私信息泄露(C1)指移动APP用户本人的不当操作或行为导致信息泄露。该指标体系下设10个二级指标:移动APP关联使用(C11)指的是用户将多个APP关联使用,或者在同一APP上关联使用不同的账号,并接收其他账号收到的消息,导致信息的泄露;用户的错误操作(C12)指用户的某些错误的操作导致信息的泄露;移动APP密码设置过于简单(C13)指用户为了便于记忆将密码设置得过于简单,很容易被破解,造成信息泄露;账号解绑或更换不及时(C14)指之前的账号不再使用,但是用户并未将原有账号解绑或更换为新账号,最常见的表现就是以手机号码为账号时,手机号不用了但并未在绑定该手机号码的APP上进行解绑,如果该账号被他人重新使用,便造成了原账号主人信息的泄露;不良的网络使用习惯(C15)指用户在上网时养成的一些不好的使用习惯,如随意点开不明链接,可能使手机感染病毒,导致信息泄露;移动设备丢失(C16),相对于固定位置的设备(如电脑等)来说,移动设备有更大的丢失风险,一旦丢失,所有的隐私信息都暴露在危险中;对隐私信息的态度过于乐观(C17)指对于移动APP对个人隐私信息的保护情况过于乐观,愿意或随意披露自己的各种信息;长期不关闭移动定位功能(C18)指的是因为移动设备的移动性与便利性,许多APP要求手机开启定位功能,例如:滴滴打车、高德地图等,人们通常在需要时开启了移动定位功能,之后却忘记关闭,这样可能导致用户位置或轨迹信息的泄露;上传过多隐私数据至网盘(C19),因移动设备的存储量相对较小,所以人们习惯于将各种个人信息或文件上传至网盘进行保存,若网盘的安全受到威胁,那么个人隐私或重要文件信息都可能会泄露;不使用移动隐私控制功能(C110),移动设备或移动APP为了防范个人隐私泄露的风险,设计了一些防止隐私泄露的功能,例如键盘锁、异地登录验证等,但许多人为了平时方便、快捷地使用移动APP而关闭了这些功能,这种行为为个人隐私信息的安全埋下了隐患。

2.2.2 移动APP平台原因导致用户隐私信息泄露 移动APP平台原因导致隐私信息泄露(C2)是指移动APP平台的运营方建设运营过程中导致APP用户个人隐私信息的泄露。该原因下设的评价指标包括10个二级指标:移动APP功能设置不合理(C21)指APP本身的功能设置存在缺陷,对于用户的隐私保护不利,如QQ软件的对于QQ空间动态的默认设置是好友与非好友都可见,发送出去的信息不仅所有人都能看到,而且可能被"二次传播",最后可能造成用户无法控制的情况;移动APP平台开放性太强(C22)指APP对于"第三方平台"的开放性太强,如某些APP为提高合作水平,在APP的使用界面推荐其他的网络平台,当用户浏览这些被推荐的网络平台时,就可能泄露自己的信息;移动APP请求授予权限过多(C23)指每个移动APP在下载时都会申请授权,例如读取通话记录、短信记录等,有些软件甚至会获取二三十项授权,其实其中很多权限是没必要获取的,而且与电脑等传统的设备相比,移动设备特有的电话通讯功能决定了其包含了大量通话记录、短信、联系人信息等,这些信息一旦泄露,后果会很严重;移动APP不经用户的同意将信息共享(C24)指APP平台不经用户同意就将用户的个人信息共享,造成用户的隐私泄露;移动APP不经用户允许修改其隐私信息(C25)指用户在上传自己的个人信息后,移动APP平台为达到自己的目的随意更改其信息;移动APP平台内部人员恶意泄露信息(C26)指的是APP平台管理不善,内部人员私自将用户信息泄露;移动APP平台内部人员滥用信息(C27)指APP平台内部人员拿出用户的个人信息为自己所用,如私自利用某用户的姓名、电话、身份证号等信息进行其他业务的办理,从而可能会给用户带来损失;移动APP平台工作人员操作失误(C28)即APP运营方工作人员由于业务流程不熟等原因产生的错误操作,造成用户隐私的泄露;移动APP风险防范技术不过关(C29)指的是移动APP平台的技术存在缺陷,导致用户在APP平台上传的某些信息被监视、窃听、盗取或破坏;行业自律性不够好(C210)指的是整个行业对于用户隐私保护都未引起重视,甚至用户个人隐私信息交易已经成为"常态"。

2.2.3 管理方原因导致用户隐私信息泄露 管理方原因导致隐私信息泄露(C3)指移动APP相关的管理机构或部门的某些原因造成移动APP用户隐私信息可能泄露的情况,包括5个二级指标:基于法律或制度要求被迫披露(C31)指为了更好地管理各种移动APP,一些法律或制度要求APP平台必须披露某些必要的注册用户个人信息,这也可能会造成用户信息的

泄露;网络隐私信息披露标准不完善(C32)指我国目前还没有一套完善的网络用户隐私信息披露标准,以至于行业内用户个人信息的披露情况十分混乱,对用户的个人隐私安全不利;监管与惩戒体系缺乏(C33)指的是没有完善的监管、惩戒体系来约束行业的行为,导致隐私信息泄露的问题日趋严重;管理机构直接将信息共享(C34)即管理机构因一些政策或规定的要求直接将存储在管理部门的某些用户个人信息共享,造成用户的隐私泄露;管理机构人员泄露(C35)指管理机构管理不善或工作人员错误操作导致用户的信息泄露。

2.2.4　其他原因导致隐私信息泄露　其他原因导致隐私信息泄露(C4)是指除上述 3 个原因(用户自身、APP 平台、管理方原因)以外的原因,包括 5 个二级指标:备份资料(C41)指每个 APP 平台都会对重要的用户信息进行备份以防服务器崩溃或瘫痪导致信息的丢失,那么这些不知何时才会删除的备份资料也成为了一种用户隐私信息安全的威胁;陌生无线网络的不安全性(C42)指的是由于移动的特性,人们可能会在不熟悉的地方使用需要网络的移动 APP,若此时移动设备本身没有足够的移动网络,就需要暂时连接陌生的无线网络,如连接了不安全的 WiFi,就可能会使个人隐私泄露;黑客攻击(C43)即网络黑客利用技术优势,通过窃取网络服务器等方式,盗取用户隐私信息;从第三方平台购买隐私信息(C44)即某些个人或机构出于自己的需要,向一些保留或管理用户隐私信息的第三方平台购买用户的信息;破解或猜测账号密码(C45)指的是某些人依据背景信息猜测他人密码或凭借技术破解他人密码,以窃取他人个人信息。

2.3　德尔菲法优化后的评价指标体系

为了保证风险评价体系的科学性与合理性,本研究又运用德尔菲法向相关专家征询意见,根据专家意见对初步构建的指标体系进行修改和完善,删除掉重要程度相对来说较低或者被其他因素包含的一些指标:C14、C22、C25、C27、C28、C35、C45,使得评价体系更加精简,最终评价体系见表 1。

表 1　移动 APP 用户隐私泄露风险评价指标体系

一级指标	二级指标
C1 用户原因导致隐私信息泄露	C11 移动 APP 关联使用
	C12 错误操作
	C13 移动 APP 密码设置简单
	C15 不良网络使用习惯
	C16 移动设备丢失
	C17 对隐私信息的态度过于乐观
	C18 长期不关闭移动定位功能
	C19 上传过多隐私数据至网盘
	C110 不使用移动隐私控制功能
C2 移动 APP 平台(运营方)原因导致隐私信息泄露	C21 移动 APP 功能设置不合理
	C23 移动 APP 请求授予权限过多
	C24 移动 APP 不经用户许可将信息共享
	C26 移动 APP 内部人员恶意泄露信息
	C29 移动 APP 风险防范技术不过关
	C210 行业自律性不够好
C3 管理方原因导致隐私信息泄露	C31 基于法律或制度要求被迫披露
	C32 网络隐私信息披露标准不完善
	C33 监管与惩戒体系缺乏
	C34 管理机构直接将信息共享
C4 其他原因导致隐私信息泄露	C41 备份资料
	C42 陌生无线网络的不安全性
	C43 黑客攻击
	C44 从第三方平台购买隐私信息

3　评价指标权重计算

3.1　基于 ANP 法的主观权重计算

ANP 又称网络分析法,是层次分析法(AHP)的拓展。ANP 适用于要素之间相互依存、影响、反馈的系统,更切合实际。因此,本文采用 ANP 法来计算各风险指标的权重是更合理的。

在 ANP 模型中指标因素被分为控制层和网络层两部分。在本文中,控制层为移动 APP 用户隐私泄露风险,网络层包括用户原因导致信息泄露、APP 平台运营方原因导致信息泄露、管理方原因导致信息泄露和其他原因导致信息泄露 4 个元素组。

因该计算过程较复杂,所以本文使用 Super Decisions 软件进行指标权重的计算,步骤为:首先确定各元素组之间的相互影响关系,然后构造判断矩阵,最后计算出各指标的权重。

3.2　基于熵权法的客观权重计算

熵可用来衡量事物出现不确定性的概念[24],信息熵理论认为,信息是对系统有序状态的度量,而熵是系统无序状态的度量。一般来说,如果某项指标的信息熵越小,表示该指标所提供的信息量越大,在综合评价中起的作用也越大,故权重也越大;反之则越小。

由于 ANP 计算得出的权重是带有一定主观色彩的,而熵权法可在一定程度上客观地计算出各项指标权重大小,对 ANP 计算出的主观权重进行修正,使得最后的结果更合理。熵权法计算权重的步骤如下:

第一步,根据专家评分表构造判断矩阵 R =

$(r_{ij})_{m\times n}$,并对矩阵中的数据进行标准化得到 Y_{ij},那么有

$$y_{ij}=\frac{r_{ij}-\min(r_i)}{\max(r_i)-\max(r_i)} \qquad 公式(1)$$

对标准化后的矩阵进行归一化处理,假设归一化后的矩阵为 X_{ij},那么

$$x_{ij}=\frac{y_{ij}}{\sum_{i=1}^{m}y_{ij}} \qquad 公式(2)$$

第二步,计算各指标的信息熵,假设第 j 项指标的信息熵为 e_j,则

$$e_i=-\frac{1}{\ln n}\sum_{i=1}^{m}x_{ij}\ln x_{ij} \qquad 公式(3)$$

并且当 $x_{ij}=0$ 时,$x_{ij}\ln x_{ij}=0$。

第三步,确定各指标权重 v_j:

$$v_j=\frac{1-e_j}{\sum_{j=1}^{n}(1-e_j)} \qquad 公式(4)$$

3.3 组合权重计算

结合相关文献[25]并考虑本文中应用方法的具体情况,可利用最小信息熵原理和拉格朗日乘子法计算出组合权重 w_j:

$$w_j=\frac{(u_jv_j)^{0.5}}{\sum_{j=1}^{n}(u_jv_j)^{0.5}} \qquad 公式(5)$$

4 实证分析

4.1 样本选取

以移动社交类 APP 用户为研究对象,进行移动 APP 用户隐私信息泄露风险评价。选择社交类 APP 的原因,是因为目前该类 APP 是使用最广泛的一类 APP,用户可以使用的移动终端为手机或平板电脑等,安卓系统与 iOS 系统的手机均可下载,而且该 APP 在两种系统的手机中的使用方法与功能基本相同。移动社交 APP 大致可分为 3 类,分别是:①传统 SNS 类,例如新浪微博、腾讯微博、人人网等;②陌生人交友类,例如陌陌、探探等;③即时通讯类,例如微信、QQ 等[26]。为了使样本的选择具有代表性和普遍性,本文综合 2018 年苹果 iTunes(中国区)与安卓应用商店给出的移动社交 APP 排行榜,每种分类各选择排名靠前的一个以及排名相对靠后的一个,共选出 6 个典型的移动社交 APP:新浪微博、兴趣部落、陌陌、派派、微信、米聊,并通过专家打分的形式对移动 APP 用户隐私泄露风险水平进行判断,分值范围为 1-10 分,分值越高表示该项指标对应的风险水平越高。为了能更加客观、科学地进行实证研究,本研究选择 8 位专家进行问卷调研及访谈,这 8 位专家中有 4 位是有着较丰富经验的从事互联网开发的专业人员,4 位是从事移动 APP 研究的学者,职称均在副教授以上。表 2 是 8 位专家对各个指标的评分结果:

表 2 专家评分

指标	专家 1	专家 2	专家 3	专家 4	专家 5	专家 6	专家 7	专家 8
C11	8	9	6	7	7	5	4	9
C12	4	4	5	4	2	5	4	4
C13	3	5	5	4	4	4	2	4
C15	10	9	7	5	9	6	8	4
C16	5	4	8	7	6	8	6	5
C17	8	7	10	6	4	4	3	9
C18	4	5	4	3	6	7	6	4
C19	3	6	5	5	5	4	5	6
C110	4	5	5	8	6	5	6	3
C21	5	8	7	10	6	9	9	7
C23	4	5	4	2	5	4	4	4
C24	4	4	4	5	2	4	4	4
C26	5	7	6	8	7	7	8	9
C29	7	8	7	9	6	6	5	8
C210	4	5	4	2	4	5	4	4
C31	3	6	4	5	5	5	4	5
C32	8	7	9	6	6	9	4	5
C33	7	5	8	7	8	9	10	6
C34	3	4	5	5	3	1	4	4
C41	4	5	5	4	4	5	2	4
C42	7	7	5	5	6	3	5	5
C43	9	8	5	9	5	4	6	7
C44	9	10	5	7	4	5	9	5

4.2 评价过程

4.2.1 熵权法确定客观权重　通过公式(1)、(2),对原始矩阵进行标准化及归一化处理,可得矩阵如下:

$$\begin{pmatrix}
0.1739 & 0.1250 & 0.0667 & 0.2308 & 0.0588 & 0.1852 & 0.0667 & 0.0000 & 0.0556 & 0.0000 & 0.1250 & 0.1333 & 0.0000 & 0.1250 & 0.1250 & 0.0000 & 0.1818 & 0.1000 & 0.0952 & 0.1176 & 0.2105 & 0.2381 & 0.2273 \\
0.2174 & 0.1250 & 0.2000 & 0.1923 & 0.0000 & 0.1481 & 0.1333 & 0.2000 & 0.1111 & 0.1429 & 0.1875 & 0.1333 & 0.1176 & 0.1875 & 0.1875 & 0.2308 & 0.1364 & 0.0000 & 0.1429 & 0.1765 & 0.2105 & 0.1905 & 0.2727 \\
0.0870 & 0.1875 & 0.2000 & 0.1154 & 0.2353 & 0.2593 & 0.0667 & 0.1333 & 0.1111 & 0.0952 & 0.1250 & 0.1333 & 0.0588 & 0.1250 & 0.1250 & 0.0769 & 0.2273 & 0.1500 & 0.1905 & 0.1765 & 0.1053 & 0.0476 & 0.0455 \\
0.1304 & 0.1250 & 0.1333 & 0.0385 & 0.1765 & 0.1111 & 0.0000 & 0.1333 & 0.2778 & 0.2381 & 0.0000 & 0.2000 & 0.1765 & 0.2500 & 0.0000 & 0.1538 & 0.0909 & 0.1000 & 0.1905 & 0.1176 & 0.1053 & 0.2381 & 0.1364 \\
0.1304 & 0.0000 & 0.1333 & 0.1923 & 0.1176 & 0.0370 & 0.2000 & 0.1333 & 0.1667 & 0.0476 & 0.1875 & 0.0000 & 0.1176 & 0.0625 & 0.1250 & 0.1538 & 0.0909 & 0.1500 & 0.0952 & 0.1176 & 0.1579 & 0.0476 & 0.0000 \\
0.0435 & 0.1875 & 0.1333 & 0.0769 & 0.2353 & 0.0370 & 0.2667 & 0.0667 & 0.1111 & 0.1905 & 0.1250 & 0.1333 & 0.1176 & 0.0625 & 0.1875 & 0.1538 & 0.2273 & 0.2000 & 0.0000 & 0.1765 & 0.0000 & 0.0000 & 0.0455 \\
0.0000 & 0.1250 & 0.0000 & 0.1538 & 0.1176 & 0.0000 & 0.2000 & 0.1333 & 0.1667 & 0.1905 & 0.1250 & 0.1333 & 0.1765 & 0.0000 & 0.1250 & 0.0769 & 0.0000 & 0.2500 & 0.1429 & 0.0000 & 0.1053 & 0.0952 & 0.2273 \\
0.2174 & 0.1250 & 0.1333 & 0.0000 & 0.0588 & 0.2222 & 0.0667 & 0.2000 & 0.0000 & 0.0952 & 0.1250 & 0.1333 & 0.2353 & 0.1875 & 0.1250 & 0.1538 & 0.0455 & 0.0500 & 0.1429 & 0.1176 & 0.1053 & 0.1429 & 0.0455
\end{pmatrix}$$

通过公式(3)确定各指标的信息熵后,由公式(4)即可计算出权重 v_j, v_j = (0.0462 0.0303 0.0360 0.0493 0.0509 0.0621 0.0544 0.0360 0.0465 0.0469 0.0303 0.0290 0.0408 0.0476 0.0303 0.0388 0.0494 0.0461 0.0331 0.0307 0.0367 0.0575 0.0714)。

4.2.2 ANP 确定主观权重 在使用 Super Decisions 软件进行计算时,首先确定各元素组之间的相互影响关系,如图 1 所示,图中箭头表示影响关系。以 C1 元素组为例,该元素组会对自身有影响,比如用户的某项错误操作可能会导致他接下来的每一项操作都是错误的,而且 C1 元素组也会对 C4 元素组造成影响,比如用户的不良网络使用习惯会使得黑客的非法攻击变得更容易,会造成更多非法分子盗取隐私信息的现象。

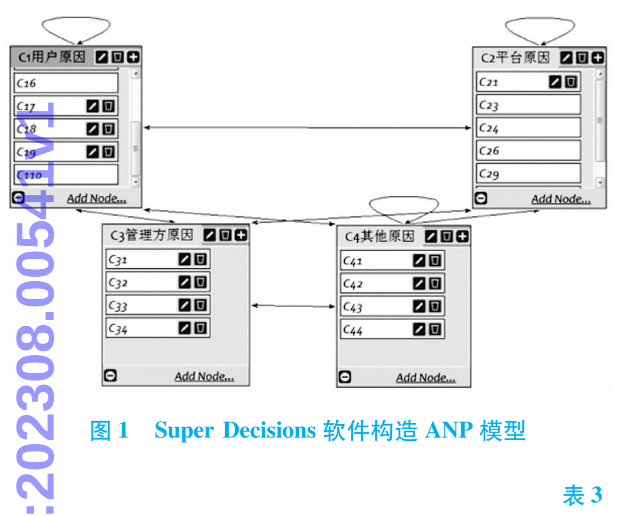


图 1 Super Decisions 软件构造 ANP 模型

然后在该软件中构造判断矩阵,如图 2 所示,以 C2 元素组为主准则,以 C23 元素为次准则,对 C2 元素组中的元素进行两两比较,以打分的形式判断重要程度,比如,这种情况下 C21 元素比 C24 元素更重要,相对重要程度为 5。

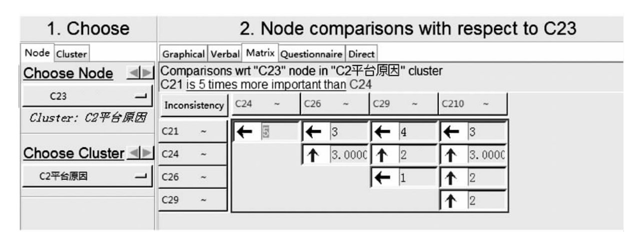


图 2 Super Decisions 软件打分结果界面

重复进行上个步骤,直到给出所有的判断矩阵,然后即可得出权重 u_j:

u_j = (0.0215 0.0153 0.0214 0.0261 0.0387 0.0450 0.0127 0.0202 0.00950.0798 0.1049 0.0508 0.0794 0.1238 0.0677 0.0199 0.0495 0.0877 0.0102 0.0200 0.0225 0.0264 0.0475)。

4.2.3 确定组合权重 按照公式(5)计算出组合权重 w_j,结果如表 3 所示:

表 3 指标权重

一级指标	二级指标	u_j	v_j	w_j	元素组组合权重
C1 用户原因导致信息泄露	C11 移动 APP 关联使用	0.0215	0.0462	0.0337	0.3088
	C12 错误操作	0.0153	0.0303	0.0231	
	C13 移动 APP 密码设置简单	0.0214	0.0360	0.0297	
	C15 不良网络使用习惯	0.0261	0.0493	0.0385	
	C16 移动设备丢失	0.0387	0.0509	0.0476	
	C17 对隐私信息的态度过于乐观	0.0450	0.0621	0.0567	
	C18 长期不关闭移动定位功能	0.0127	0.0544	0.0281	
	C19 上传过多隐私数据至网盘	0.0202	0.0360	0.0289	
	C110 不使用移动隐私控制功能	0.0095	0.0465	0.0225	
C2 移动 APP 平台(运营方)原因导致信息泄露	C21 移动 APP 功能设置不合理	0.0798	0.0469	0.0656	0.3591
	C23 移动 APP 请求授予权限过多	0.1049	0.0303	0.0604	
	C24 移动 APP 不经用户许可将信息共享	0.0508	0.0290	0.0412	
	C26 移动 APP 内部人员恶意泄露信息	0.0794	0.0408	0.0610	
	C29 移动 APP 风险防范技术不过关	0.1238	0.0476	0.0823	
	C210 行业自律性不够好	0.0677	0.0303	0.0486	
C3 管理方原因导致信息泄露	C31 基于法律或制度要求被迫披露	0.0199	0.0388	0.0297	0.1706
	C32 网络隐私信息披露标准不完善	0.0495	0.0494	0.0530	
	C33 监管与惩戒体系缺乏	0.0877	0.0461	0.0682	
	C34 管理机构直接将信息共享	0.0102	0.0331	0.0197	
C4 其他原因导致信息泄露	C41 备份资料	0.0200	0.0307	0.0265	0.1615
	C42 陌生无线网络的不安全性	0.0225	0.0367	0.0308	
	C43 黑客攻击	0.0264	0.0575	0.0418	
	C44 从第三方平台购买隐私信息	0.0475	0.0714	0.0624	

4.2.4 模糊综合评价法判断各 APP 风险水平高低

下面将以微信为例,展示模糊综合评价法的评价过程,表 4 为各指标权重及针对微信 APP 的专家调研结果:

表 4 指标权重及模糊综合评价法专家调研结果

一级指标	权重	二级指标	权重	专家划分为各个档次的人数				
				高风险	较高风险	中等风险	较低风险	低风险
用户原因导致隐私信息泄露	0.3088	移动 APP 关联使用	0.0337	1	1	2	3	1
		操作错误	0.0231	1	2	1	2	2
		移动 APP 密码设置简单	0.0297	2	2	2	1	1
		不良网络使用习惯	0.0385	1	3	1	2	1
		移动设备丢失	0.0476	1	2	2	2	1
		对隐私信息的态度过于乐观	0.0567	1	2	2	1	2
		长期不关闭移动定位功能	0.0281	0	2	2	3	1
		上传过多隐私数据至网盘	0.0289	0	1	2	2	3
		不使用移动隐私控制功能	0.0225	1	2	2	2	1
移动 APP 平台运营方原因导致隐私信息泄露	0.3591	移动 APP 功能设置不合理	0.0656	0	1	3	2	2
		移动 APP 请求授予权限过多	0.0604	1	2	3	1	1
		移动 APP 平台不经过用户许可将信息共享	0.0412	0	2	1	3	2
		移动 APP 平台内部人员恶意泄露信息	0.0610	1	1	2	3	1
		移动 APP 风险防范技术不过关	0.0823	0	1	4	2	1
		行业自律性不够好	0.0486	1	2	2	2	1
管理方原因导致隐私信息泄露	0.1706	基于法律或制度要求被迫披露	0.0297	0	1	2	3	2
		网络隐私信息披露标准不完善	0.0530	1	2	3	1	1
		监管与惩戒体系缺乏	0.0682	1	3	2	1	1
		管理机构直接将信息共享	0.0197	0	1	1	4	2
其他原因导致隐私信息泄露	0.1615	备份资料	0.0265	0	1	4	2	1
		陌生无线网络的不安全性	0.0308	2	3	2	1	0
		黑客攻击	0.0418	1	2	3	2	0
		从第三方平台购买隐私	0.0624	1	2	2	1	2

对表 4 数据进行计算可得模糊评判矩阵:

$$
R=\begin{pmatrix}
0.125 & 0.125 & 0.25 & 0.125 & 0.125 & 0.125 & 0 & 0 & 0.125 & 0 & 0.125 & 0 & 0.125 & 0 & 0.125 & 0 & 0.125 & 0.125 & 0 & 0 & 0.25 & 0.125 & 0.125 \\
0.125 & 0.25 & 0.25 & 0.375 & 0.25 & 0.25 & 0.25 & 0.125 & 0.25 & 0.125 & 0.25 & 0.25 & 0.125 & 0.125 & 0.25 & 0.125 & 0.25 & 0.375 & 0.125 & 0.125 & 0.375 & 0.25 & 0.25 \\
0.25 & 0.125 & 0.25 & 0.125 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.375 & 0.375 & 0.125 & 0.25 & 0.5 & 0.25 & 0.25 & 0.375 & 0.25 & 0.125 & 0.5 & 0.25 & 0.375 & 0.25 \\
0.375 & 0.25 & 0.125 & 0.25 & 0.25 & 0.125 & 0.375 & 0.25 & 0.25 & 0.25 & 0.125 & 0.375 & 0.375 & 0.25 & 0.25 & 0.375 & 0.125 & 0.125 & 0.5 & 0.25 & 0.125 & 0.25 & 0.125 \\
0.125 & 0.25 & 0.125 & 0.125 & 0.125 & 0.25 & 0.125 & 0.375 & 0.125 & 0.25 & 0.125 & 0.25 & 0.125 & 0.125 & 0.125 & 0.25 & 0.125 & 0.125 & 0.25 & 0.125 & 0 & 0 & 0.25
\end{pmatrix}
$$

根据各项指标的权重,对矩阵 R 进行模糊综合变换,可得模糊综合评价指标。

$$
B = R \cdot A = \begin{pmatrix} 0.0923125 \\ 0.2237625 \\ 0.2894875 \\ 0.2339875 \\ 0.16045 \end{pmatrix}
$$

对评判结果进行赋值,建立备择集。备择集如下:

V = {高风险,较高风险,中等风险,较低风险,低风险} = (9,7,5,3,1)

$$
p = V \cdot B = (9,7,5,3,1) \cdot \begin{pmatrix} 0.0923125 \\ 0.2237625 \\ 0.2894875 \\ 0.2339875 \\ 0.16045 \end{pmatrix} = 4.7070
$$

最后得到的综合隶属度为 4.7070。整体上说,调查研究表明该 APP 用户隐私泄露的风险程度处于较低风险和中等风险之间,更接近于中等风险。

用同样的方法可将其他几个 APP 的综合隶属度计算出来,新浪微博、兴趣部落、陌陌、派派、米聊的综合隶属度分别为:4.9110、4.8903、5.4230、5.5156、4.8534。按照隶属度大小可将各 APP 风险水平从高到

低排列：派派 > 陌陌 > 新浪微博 > 兴趣部落 > 米聊 > 微信。

4.3 讨论分析

4.3.1 一级评价指标讨论分析 结果表明，一级指标权重中最为重要的是“移动 APP 平台原因造成的隐私信息泄露风险（C2）”，其余依次为“用户原因导致的隐私信息泄露风险（C1）”“管理方原因造成的隐私泄露风险（C3）”“其他原因导致的隐私信息泄露风险（C4）”。这一数据结果表明，在移动用户隐私信息泄露风险中平台开发商应当加强平台功能设置，请求正常业务范围内的授权，同时，平台开发商内部应建立相应的用户信息保密管理制度和信息泄露的追责机制，并采取相应的安全密钥技术避免因技术原因导致外部黑客或病毒的侵犯，避免因平台原因导致的消费者隐私信息的泄露。用户应当加强隐私保护意识，谨慎披露个人信息。行业监管部门也应出台相应的行业监管体例或消费者个人隐私泄露的立法，在国家制度层面加强对平台开发商的监管。

4.3.2 二级评价指标权重分析 为了能更好地理解权重不同的各二级指标的风险程度高低，并且使管理者能够重点关注某些重要程度相对较高的风险，下面将依据各指标的权重大小对各指标进行风险等级的划分。结合相关文献[27]和移动社交类 APP 用户隐私泄露风险的具体情况，根据各项指标的组合权重结果，将二级风险指标分为 4 个等级，权重数值在 0.65 以上的为极度风险，权重数值在 0.5 - 0.65 之间的为高风险，权重数值处于 0.3 - 0.5 之间的为中等风险，权重数值在 0.3 以下的为低风险。结合评价结果，其中极度风险有 3 个，分别是“移动 APP 风险防范技术不过关”“监管与惩戒体系缺乏”“移动 APP 功能设置不合理”；高风险共有 5 个，分别是“从第三方平台购买隐私信息”“移动 APP 内部人员恶意泄露信息”“移动 APP 请求授予权限过多”“用户对隐私信息的态度过于乐观”“移动 APP 用户隐私信息披露标准不完善”。二级指标数据分析结果表明，除 APP 平台自身严格自律、改进功能并提升技术以外，为了防止用户隐私泄露现象的发生，相关部门应该出台相关政策规定，如 APP 用户隐私披露标准、请求授权标准等；同时，政府应加大对恶意隐私泄露行为的惩罚力度，规范个人隐私信息使用行为；用户也应当提高自身的隐私保护意识与警惕性。

4.3.3 移动社交 APP 用户隐私信息泄露风险分析 在所选的 6 个 APP 中，微信的用户隐私泄露风险水平最低，而派派的用户隐私泄露风险水平最高。从分类的角度来看，即时通讯类社交 APP 所处的风险等级最低，而陌生人交友类社交 APP 风险等级最高，传统 SNS 类社交 APP 风险水平处于中间位置。而且一般来说，同类型的 APP 中，使用量较高的 APP 的用户隐私泄露风险略低于使用量较低的 APP，因为一般较受欢迎的 APP 开发时间较长，建设运营经验丰富，相关的风险防范措施到位，保护用户隐私信息的意识较强，所以其风险水平相对低一些。

访谈中主要询问了各位专家认为哪些风险指标较重要、每个移动 APP 在重要指标上的表现问题等，访谈结果基本能涵盖实证分析中的大部分极度风险和重要风险指标。与问卷调研提供的数据结果相比，访谈结果的模糊性较强一些，但也能提供许多信息。例如，对于“移动 APP 功能设置不合理”，新浪微博与探探的风险表现可能略强一些，而对于“移动 APP 申请授予权限过多”，几个 APP 表现大致差不多，经查证，这 6 个 APP 获取的权限数量都在 10 个左右，确实相差很少。因此，不同的指标表现在不同的 APP 上的风险水平可能相似，也可能有很大的差别。

针对以上情况，用户应当提高自身警惕，尤其在使用陌生人交友类社交 APP 时，应当更加谨慎披露自己的个人信息，增强隐私保护意识；从 APP 的角度来看，移动 APP 平台应当提高自身实力，结合自身 APP 的特点对其功能与基本设置进行改善，并根据自身的实际情况对风险较高的指标进行重点改善，同时应当加强内部管理，提升员工整体素质与道德水平，并定期对平台的用户隐私泄露风险防范技术进行更新和改进，以保证用户隐私信息的安全。

5 研究结论

本研究的理论价值在于，依据移动 APP 用户隐私信息泄露的影响因素构建了移动 APP 用户隐私泄露风险评价指标体系，并对移动社交 APP 用户隐私信息泄露进行风险评价。论文建立了 4 个维度 23 个二级指标的指标体系，在此基础上采用 ANP 和熵权法分别确定了主观权重和客观权重，然后计算出各指标的组合权重，实现了两种方法的优势互补，从而为移动 APP 用户隐私泄露风险评价提供研究方法的支撑。

本文的实践价值在于,选择移动社交类 APP 进行实证分析。一级指标的数据分析结果表明,APP 平台原因造成的隐私泄露风险最大,其余依次是用户原因、管理方原因、其他原因造成的隐私泄露风险。二级指标数据分析结果表明,极度风险有 3 个,分别是“移动 APP 风险防范技术不过关”“监管与惩戒体系缺乏”“移动 APP 功能设置不合理”;高风险共有 5 个,分别是“从第三方平台购买隐私信息”“移动 APP 内部人员恶意泄露信息”“移动 APP 请求授予权限过多”“用户对隐私信息的态度过于乐观”“移动 APP 用户隐私信息披露标准不完善”。移动社交类 APP 实证分析结果表明,几个 APP 的风险水平高低有差别,但都接近于中等风险水平,说明用户在使用社交类 APP 时存在的隐私泄露的风险是不可忽视的,而且不同类型的社交 APP 整体风险水平也是不同的,受欢迎程度较高的 APP 风险水平相对低一些,在这种情况下,移动 APP 平台、用户、监管部门各方应共同努力,针对不同 APP 的不同情况采取相应的措施,来降低社交类 APP 用户在使用过程中的隐私泄露风险。

本文研究中,仅对社交类 6 个 APP 进行了用户隐私风险评价分析,样本选择具有一定的局限性。在后续研究中,笔者将对比分析不同类 APP 的隐私披露风险,并对每类中有代表性 APP 进行详细的对比分析。

参考文献:

[1] 罗力. 我国移动互联网用户个人信息安全风险和治理研究[J]. 图书馆学研究,2016(13):37－41.

[2] 李丽娜. 论如何加强我国隐私权的法律保护体系[D]. 延吉:延边大学,2006.

[3] 张军,熊枫. 网络隐私保护技术综述[J]. 计算机应用研究,2005(7):9－11,28.

[4] ZHU K,HE X M,XIANG B,et al. How dangerous are your smartphones? app usage recommendation with privacy preserving[J]. Mobile information systems,2016(4/5):1－10.

[5] BANSAL G, ZAHEDI F M, GEFEN D. Do context and personality matter? trust and privacy concerns in disclosing private information online[J]. Information & management,2016,53(1): 1－21.

[6] LI Y. The impact of disposition to privacy, Website reputation and Website familiarity on information privacy concerns[J]. Decision support systems,2014,57(1):343－354.

[7] MARTÍNEZ-PÉREZ B, DE LA TORRE-DÍEZ I, LÓPEZ-CORONADO M. Privacy and security in mobile health Apps: areview and recommendations[J]. Journal of medical systems,2015,39(1): 181－189.

[8] MILTGEN C L,SMITH H J. Exploring information privacy regulation, risks, trust, and behavior[J]. Information & management, 2015,52(6):741－759.

[9] 王晰巍,相甍甍,张长亮,等. 新媒体环境下信息隐私国内外研究动态及发展趋势[J]. 图书情报工作,2017,61(15):6－14.

[10] 李卓卓,马越,李明珍. 数据生命周期视角中的个人隐私信息保护——对移动 APP 服务协议的内容分析[J]. 情报理论与实践,2016,39(12):63－68.

[11] 刘娇,白净. 中外移动 APP 用户隐私保护文本比较研究[J]. 汕头大学学报(人文社会科学版),2017,33(3):82－87.

[12] 朱光,丰米宁,陈叶,等. 大数据环境下社交网络隐私风险的模糊评估研究[J]. 情报科学,2016,34(9):94－98.

[13] 王珊,李永先. 我国大数据时代个人信息保护研究综述[J]. 中国集体经济,2016(28):54－55.

[14] 孟晓明,贺敏伟. 社交网络大数据商业化开发利用中的个人隐私保护[J]. 图书馆论坛,2015,35(6):67－75.

[15] 徐晓露. 移动社交网络用户隐私安全问题及保护研究[D]. 重庆:重庆大学,2014.

[16] 张秋瑾. 云计算隐私安全风险评估[D]. 昆明:云南大学,2015.

[17] 朱义杰. 基于位置服务中的隐私泄露风险分析与评估[D]. 贵阳:贵州大学,2016.

[18] 邝青青. 基于个人隐私泄露的风险评估[D]. 贵阳:贵州大学,2016.

[19] 沈洪洲,汤雪婷,周莹. 我国移动社会化媒体隐私保护功能的可用性研究[J]. 图书情报工作,2017,61(4):23－30.

[20] 王娜,许大辰. 移动社交网络中个人信息保护现状的调查与分析——从用户行为习惯视角出发[J]. 情报杂志,2015,34(1):185－189,194.

[21] 程瑶,应凌云,焦四辈,等. 移动社交应用的用户隐私泄漏问题研究[J]. 计算机学报,2014,37(1):87－100.

[22] 齐晓娜,张宇敬,封二英. 移动社交网络用户隐私保护问题研究[J]. 产业与科技论坛,2017,16(16):35－36.

[23] 王莲芬. 网络分析法(ANP)的理论与算法[J]. 系统工程理论与实践,2001(3):44－50.

[24] 罗赟骞,夏靖波,陈天平. 网络性能评估中客观权重确定方法比较[J]. 计算机应用,2009,29(10):2624－2626,2631.

[25] 郑晓云,王雨. 基于 AHP 和熵权法的房地产开发企业诚信评价[J]. 山西建筑,2016,42(2):213－214.

[26] 王树义,朱娜. 移动社交媒体用户隐私保护对策研究[J]. 情报理论与实践,2013,36(7):36－40.

[27] 李明高. 信息安全风险评估在信息安全体系建设中的应用分析[J]. 电脑与电信,2009(1):83－85.

作者贡献说明:

田波:提出研究思路及框架,撰写及修改论文;
郑羽莎:撰写及修改论文;
刘鹏远:负责数据的采集、整理和计算;
李春好:负责指标体系的确立与分析。

The Evaluation Index and Empirical Study on Risk of Privacy Information Disclosure of Mobile APP Users

Tian Bo Zheng Yusha Liu Pengyuan Li Chunhao
School of Management, Jilin University, Changchun 130022

Abstract: [**Purpose/significance**] Aiming at the increasingly serious privacy information leakage of mobile APP users, this paper analyzes and evaluates the disclosure risks of privacy information and provides suggestions for risk response, which helps to protect the privacy of mobile APP users and promote the healthy development of information platform. [**Method/process**] This paper analyzes the risk of privacy information disclosure of mobile APP users and constructs the index system of risk assessment of users' privacy information disclosure. It uses the analytic network process (ANP) and entropy method to synthetically determine the index weight of portfolio. Finally this paper applies the fuzzy comprehensive evaluation method to make an empirical analysis of mobile social networking APPs. [**Result/conclusion**] The mobile APP user privacy information disclosure evaluation index system has certain scientificalness and practicality. Among the index system, the APP platform reason has the highest risk of privacy disclosure and the users reason secondly. On the whole, Paipai has the highest users' risk of privacy leaks and WeChat has the lowest risk, but all are close to medium risk. In order to reduce the risk of privacy information disclosure of mobile social APP users, mobile users, APPs and regulatory authorities should focus on the different situations of different APPs and take measures with emphasis.

Keywords: mobile APP users privacy information information disclosure risk assessment analytic network process entropy method fuzzy comprehensive evaluation method